# Work From Home Security Tips for Individuals

## Introduction

Working from home can present some unique challenges to your daily operations, and it's important to keep in mind the security of your home network and the devices that connect to it. Here are some things you can do to help maintain a secure working environment.

## Keep Your Home Computers and Devices Secure

If you or your housemates have personal computers or devices connected to your home network, maintain a sound security posture and follow good security practices such as:

**Embrace multi-factor authentication (MFA)**

Username/password authentication is no match for any adversary, much less a determined one. Set up MFA on all your accounts. Especially consider your email, personal and professional social media, bank & investment accounts, healthcare accounts, insurance accounts, etc.

**Maintain updates**

Making sure your computer has the latest updates and patches is one of the most important ways to protect yourself and your data. Perform the following steps to install the latest patches and updates.

- For PC's
  - Start -> Settings -> Update and Security -> Check for updates
- For Macs
  - Apple menu -> System Preferences -> Software Update
- For Tablets & Mobiles
  - Each are slightly different, but find your device *Settings* then look for *Updates*
- Don't forget to update apps on these devices as well

**Safe surfing**

The Internet grants us access to a wealth of information, people and technology. However, there are unsafe parts of the Internet. Take care to avoid these parts.

- Consider the sites you and your housemates visit. Choose reputable sources for information, and type in the address yourself. There are a lot of sites out there, especially now, that are trying to prey on our interest for more information and fear.
- Be selective about the applications you download and only download from reputable vendors.

**Phishing awareness**

Just like with Safe Surfing, there are a lot of phishing scams flourishing now. Don't be a victim! Be suspicious about any links that are sent to you. If you're interested in donating to a cause, go directly to that cause and then find their donation link. If you have *any* doubt, don't click the link. Teach your housemates about phishing and encourage them to be vigilant as well.

# Work From Home Security Tips for Individuals

## Secure Your Router

Many routers come with settings that make it easy to connect. Unfortunately, that often means we rely on the default configuration and administrator credential. Here are some steps you can take to help protect your network. Your provider's support site or helpdesk can help you navigate these technical changes.

**Connect to your router**

Most routers have an IP address/admin URL. If you don't know it, look on the back of your router. If there's nothing there, Google the model of router and the phrase *admin URL*. You will likely also find the default password this way. If all else fails, contact your provider for help.

Here are some safe networking considerations:

- Change default WiFi router password – many have a basic username and password.
- Turn on encryption (WPA2 or WPA3) – this makes it harder for people to snoop on your communication and helps control who can connect to your WiFi.
- Disable remote management – many routers can be logged into from the internet. You want to turn that off.
- Disable WPS (Wi-Fi Protected Setup or Wi-Fi Simple Config) – a simple but vulnerable method of connecting devices to your router.
- Disable UPnP (Universal Plug and Play) – another simple but vulnerable way to connect devices.
- Monitor your network for unknown devices – if you don't recognize a device, you can terminate their connection in the router admin portal.
- Create a separate guest network for visitors – friends of housemates can still use your WiFi but will be separated from your use.

## Protect Your Data

With everyone at home, it can be challenging to keep things private. Here are some things to consider:

- Lock your screen when away.
- Be aware of shoulder surfing – protect your data from prying eyes.
- Hold sensitive conversations in private. Don't be afraid to ask for privacy.
- Print only if absolutely necessary. Cross cut shred for disposal or maintain the documentation under lock and key until you can bring it to shred bins.